5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 03/30/2007
BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/771,967	AKKAR ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submissions filed on 27 December 2005 and 16 January 2007 have been entered. The submission of 27 December 2005 accompanied a petition to revive the present application under 37 CFR 1.137(b), such petition being granted on 17 March 2006. The request for continued examination included a request for a suspension of action under 37 CFR 1.103(c). No further responses were submitted during the period of suspension of action. The submission filed on 27 December 2005 was considered non-compliant under 37 CFR 1.121 for the reasons set forth in the notice of non-compliant amendment mailed 19 December 2006. Applicant filed the reply of 16 January 2007 in response to the notice of non-compliant amendment.

2. By the reply received 16 January 2007, Claims 14-26 and 31-33 have been amended. No claims have been added or canceled. Claims 14-33 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 16 January 2007 have been fully considered but they are not persuasive.

Claims 14-33 were rejected under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Kocher et al, US Patent 6278783, and Chow et al, US Patent 6594761. The Examiner notes that the grounds of rejection are slightly altered below, to a rejection under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783; however, because the rejection refers to the same prior art, Applicant's arguments are addressed herein.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Kocher does not meet the claims of the present application (page 14 of the present response) and that Chow does not disclose determining whether or not the complement is to be performed based on a random determination (page 15 of the present response). However, Kocher is relied upon for a teaching of determining what operation to perform based on a random determination (column 9, lines 1-13 as cited), and in combination with the disclosure of Chow, this suggests determining whether the complement of an operation is to be performed based on a random determination.

In response to applicant's argument that there is no suggestion to combine the references (page 15 of the present response), the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to include the teachings of Chow was, as cited, to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9), and the motivation to further include the teachings of Kocher was, as cited, to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9). Although Applicant alleges that there are not teachings that would suggest modification of the prior art to one of ordinary skill in the art (page 15 of the present response), the Examiner notes that Applicant also acknowledges that increasing tamper resistance or leak minimization are in fact disclosed (i.e. taught) as objects of Kocher and Chow. The Examiner recognizes that the teachings of the prior art are one of the three possible sources for motivation to combine references. See MPEP § 2143.01 I. Further, the strongest rationale for combining references is a recognition, for example, in the prior art, that some advantage or expected beneficial result would have been produced by the combination. See MPEP § 2144. The fact that the disclosed inventions of Kocher and Chow have the above-noted objects at the very least suggests that those objects would be a beneficial result or advantage of using the teachings disclosed therein.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Objections

4. The objection to Claim 14 for informalities is withdrawn in light of the amendments to the claim.

5. Claim 16 is objected to because of the following informalities:

Claim 16 recites the limitation "intermediate result obtained on carrying out" in line 5 of the claim. It appears that "on" is intended to read "by".

Appropriate correction is required.

6. Applicant is advised that should claim 23 be found allowable, claim 32 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 14-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 14-33 are directed to methods of performing a cryptographic protocol. However, these methods are directed merely an abstract idea, and not to a practical application of that abstract idea. In particular, independent Claim 14 is directed to a method that has as its final step a comparison between a resultant message and a result. For a method to be directed to a practical application, it must either produce a physical transformation or a useful, concrete, and tangible result. The method clearly does not produce a physical transformation. Further, the method does not produce a useful, concrete, and tangible result. Although the result of the comparison is useful as described in the present specification, and is also concrete, the result is not tangible. That is, it is merely an abstract result; the comparison is not actually used to perform any further computation or transformation. See MPEP § 2106.01 IV. It is additionally noted that none of the dependent claims produce any further useful, concrete, and tangible result that would define a practical application.

Claim Rejections - 35 USC § 112

9. The rejection of Claims 14-33 under 35 U.S.C. 112, second paragraph is NOT withdrawn. Although the amendments to the claims have remedied some issues of indefiniteness, the amendments have also raised new issues of indefiniteness, and other issues noted in the previous Office action have not been addressed.

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 14-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 14 recites the limitation "the second chain of operations comprising some operations of the first chain of operations which are performed in the same state and some other operations of the first chain of operations which are performed in a complemented state". The use of the term "some" renders the claim indefinite, because it does not clearly define any specific and definite quantity, nor does it set forth a specific numerical range or provide a definite basis of comparison for determining such a quantity. Further, the step of "selecting to output as the resultant message, depending on the step of randomly selecting, one of either a last operation of the second chain of operations in a same state or the last operation of the second chain of operations in a complemented state" is generally unclear, as it is not clear how the last operation (in either the same or complemented state) is output as the resultant message. It appears that it is intended that the result of the last operation is to be output as the resultant message.

Claims 15-19, 23, 27, 28, and 31 each recite the limitation "the at least a part of the first chain of operations". There is insufficient antecedent basis for this limitation in the claims, as it is not clear whether this refers to the at least part of the operations of the first chain of operations in a same state, or the at least a part of the first chain of operation in a complemented state (see lines 17-20 of Claim 14).

Claims 16 and 19 further recite the limitation "carrying out said second chain of operations until the operation" of permutation or transfer, respectively. It is not clear exactly what is meant by the phrase "until the operation".

Claim 20 recites the limitation "a series of several parts" in line 5; however, line 8 refers to "either such part", which appears to refer to only two such parts. This appears to be inconsistent with the number of "each of a series of several parts", as that limitation can refer two more than two parts. This inconsistency renders the claim indefinite.

Claim 21 recites the limitation "wherein the step of randomly selecting comprises identifying a series of operations within each of said series of several parts of the first chain of operations, comprises randomly selecting..." This is generally unclear and narrative, and appears to be missing a link between the clauses.

Claims 22 and 23 each recite the limitation "each such part of the first chain of operations". It is not clear how the term "such" is intended to modify each part, or to what such is intended to refer.

Claim 22 further recites the limitation “the step of selecting to output as the resultant message is decided depending on the state of the complementation counter”. This is generally unclear, as it is not clear what exactly is decided in reference to the step of selecting.

Claim 23 further recites the limitation “deciding the step of outputting the resultant message”. This is also generally unclear because it is not clear what exactly is decided in reference to the step of outputting.

Claim 24 recites the limitation “when an operation of the first chain of operations was performed in the same state as in the first chain of operations”. It appears that this refers to every time the operation is performed; since the operation is **in** the first chain of operations, it **must** be performed in the same state as in the first chain of operations. Further, Claim 24 recites the limitation “the computing of a parameter” and “the decision to perform”. There is insufficient antecedent basis for these limitations in the claims. Further, the claim refers to an operation of the first chain of operations being performed. It is unclear whether this is intended to refer to the first chain of operations being performed when applied within the first entity, or to the at least a part of the operations that can be selected in the step of determining the second chain of operations to be applied within the second entity.

Similarly, Claim 25 recites the limitation “to perform either the whole of the first chain of operations in the same state as in this first chain of operations”. However, it is not clear how operations that are **in** the first chain of operations can be performed in any state other than the same state as in the first chain of operations.

Claim 26 refers to an operation of the first chain of operations being performed. It is unclear whether this is intended to refer to the first chain of operations being performed when applied within the first entity, or to the at least a part of the operations that can be selected in the step of determining the second chain of operations to be applied within the second entity. Further, the claim refers to "such operations" in line 6 of the claim; however, it is not clear exactly to which operations this is intended to refer.

Claim 31 recites the limitation "selecting to output as the resultant message is decided depending on the state of the complementation counter". This is generally unclear, as it is not clear what exactly is decided in reference to selecting to output.

Claim 32 recites the limitation "deciding the step of outputting the resultant message". This is also generally unclear because it is not clear what exactly is decided in reference to the step of outputting.

Claims 33 recites the limitations "the computing of a parameter", and "the decision to perform". There is insufficient antecedent basis for these limitations in the claims. Further, the claim refers to an operation of the first chain of operations being performed. It is unclear whether this is intended to refer to the first chain of operations being performed when applied within the first entity, or to the at least a part of the operations that can be selected in the step of determining the second chain of operations to be applied within the second entity.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 14-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 14, Applicant admits as prior art a method including applying a message to first and second electronic entities, applying a first chain of operations to the message within the first entity to obtain a result, applying a second chain of operations to the message within the second entity to obtain a resultant message, and comparing the resultant message to the result (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly selecting to perform operations of the first chain in either a normal or a complemented state.

Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-

column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 20 and 21, Chow further discloses that a decision whether to perform an operation or its complement is made for each operation (column 18, line 65-column 19, line 13).

In reference to Claims 22 and 31, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and a counter is updated (column 9, lines 25-27).

In reference to Claims 23 and 32, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and intermediate responses are transmitted (see column 2, lines 17-19).

In reference to Claims 24, 26, and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30).

In reference to Claim 25, Kocher further discloses two chains of operations (column 6, lines 28-38 and 64-67).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER